UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,070	02/01/2002	Satyendra Yadav	10559-754001	2485

20985 7590 12/10/2008

FISH & RICHARDSON, PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
TRUVAN, LEYNNA THANH	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
12/10/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Office Action Summary	Application No.	Applicant(s)	
	10/066,070	YADAV, SATYENDRA	
	Examiner	Art Unit	
	Leynna T. Truvan	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 September 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21-28* is/are pending in the application.

4a) Of the above claim(s) *1-20 and 29-30* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 21-28 are pending.

Claims 1-20 and 29-30 are cancelled.

Response to Arguments

2. Applicant's arguments filed 9/22/08 have been fully considered but they are not persuasive.

Regarding the argument on pg.5, that Kouznetsov does not teach obtaining application-specific intrusion criteria. Applicant states the Kouznetsov discloses:

> The sequence of the execution of the monitored events is tracked for each of the applications. Each occurrence of a specific event sequence characteristic of computer virus behavior and the application that performed the specific event sequence, are identified. A histogram describing the specific event sequence occurrence for each of the applications is created. Repetitions of the histogram associated with at least one object are identified.
>
> The process identifier (ID) 71 and application name 72 fields respectively store the process number and name of the application 33, 34, 35 (shown in FIG. 2) to which the recorded monitored event is associated.
>
> ... records for the monitored events 70 are retrieved for each of the applications 33, 34, 35 (block 151).

The underlined citation above reads on the claimed application-specific intrusion criteria that were tracked for each application as monitored events. Applicant later acknowledges on pg.6, that (col.2, lines 51-58 and col.5, lines 9-12 and col.7, lines 1-2)the monitored events are then analyzed to determine whether the application is performing a sequence of suspicious actions characteristic of computer viruses (col.2, lines 32-40 and col.4, lines 15-36). This clearly shows obtaining intrusion criteria that are specific to an application.

Regarding the argument on pg.6, that neither Kouznetsov nor Gryaznov teaches or suggests the claimed examining a set of instructions embodying an invoked application to

identify the invoked application. Kouznetsov as noted above teaches and suggests the application specific intrusion criteria by determinining whether the application is performing a sequence of suspicious actions characteristic of computer viruses (col.2, lines 32-40 and col.4, lines 15-36). A (intrusive) criteria broadly and obviously can be any data/content that is considered to identify or measure what is deemed as intrusive or as an intrusion. In essence, examiner finds Kouznetsov suggest identifying an invoked application. However, examiner goes further to give the claimed "to identify the invoked application" can also be a form of literal identification or labeling the intrusion (i.e. as ID, name, number, etc.) so as "to identify the invoked application" of the intrusion criteria specific to an application. Hence, Gryaznov is combined with Kouznetsov to teach the obviousness of identifying the invoked application. Gryaznov discloses a method and system for providing computer malware names from multiple anti-virus scanners (col.1, lines 6-9) where an anti-virus scanner detect and identify viruses and other malwares (col.4, lines 7-10 and col.6, lines 5-15). The information identifying the computer malware may comprise a name of the computer malware and at least one of a computer virus, a computer worm, or Trojan horse program (col.2, lines 7-15). Hence, Gryaznov reads on the claimed identifying the invoked application, obtaining application-specific intrusion criteria and monitoring network communications for the invoked application, after the examining and the obtaining, using the application-specific intrusion criteria to detect an intrusion (col.2, lines 1-55). It would have been obvious for a person of ordinary skills in the art to combine the teachings of Kouznetsov with Gryaznov for identifying the invoked application because different anti-virus programs may call different computer malwares the same name where providing just the name of a virus is not sufficient where this takes corrective action after

a technique by which multiple names of a given virus can be determined in a quick and automated fashion (Gryaznov-col.1, lines 24-35 and 52-61). Therefore, examiner have combined proper and relevant prior arts for a person of ordinary skills in the computer technology art to read on the claimed invention.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 21-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kouznetsov (US 6,973,577), and further in view of Gryaznov (US 7,065,790).

As per claim 21:

Kouznetsov discloses a system comprising:

a network; (col.3, lines 48-55)

a security operation center coupled with the network; and (col.3, lines 41-45)

one or more machines coupled with the network (col.3, lines 46-47 and 55-59), each machine comprising a communication interface and a memory (col.3, lines 60-67) including an execution area configured to perform operations comprising examining a set of instructions embodying an invoked application (col.2, lines 47-48 and col.4, lines 12-14 and 28-47) *[to identify the invoked application]*, obtaining application-specific intrusion criteria (col.2, lines 51-58 and col.5, lines 9-12 and col.7, lines 1-2), and monitoring network communications for the

invoked application, after the examining and the obtaining, using the application-specific intrusion criteria to detect an intrusion. (col.2, lines 32-40 and col.4, lines 15-36)

Kouznetsov discloses examining a set of instructions (or program code) embodying an invoked application where each occurrence of a specific event sequence characteristic of computer virus behavior and the application that performed the specific event sequence, are identified (col.2, lines 53-59). However, did not clearly recite the claimed to identify the invoked application.

Gryaznov discloses a method and system for providing computer malware names from multiple anti-virus scanners (col.1, lines 6-9). Gryaznov discloses additional problem arises in that different anti-virus programs may call different computer malwares the same name where providing just the name of a virus is not sufficient. Thus, a need arises for a technique by which multiple names of a given virus can be determined in a quick and automated fashion (col.1, lines 52-61). Types of malware include computer viruses, Trojan horse programs, and other content (col.3, lines 7-28). Gryaznov includes an anti-virus scanner to detect and identify viruses and other malwares (col.4, lines 7-10 and col.6, lines 5-15). The information identifying the computer malware may comprise a name of the computer malware and at least one of a computer virus, a computer worm, or Trojan horse program (col.2, lines 7-15). Hence, Gryaznov reads on the claimed identifying the invoked application, obtaining application-specific intrusion criteria and monitoring network communications for the invoked application, after the examining and the obtaining, using the application-specific intrusion criteria to detect an intrusion (col.2, lines 1-55).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Kouznetsov with Gryaznov for identifying the invoked application in order to take corrective action after a technique by which multiple names of a given virus can be determined in a quick and automated fashion because different anti-virus programs may call different computer malwares the same name where providing just the name of a virus is not sufficient (Gryaznov-col.1, lines 24-35 and 52-61).

As per claim 22: See Kouznetsov on col.2, lines 53-67; discussing the application-specific intrusion criteria comprises a normal communication behavior threshold.

As per claim 24: See Kouznetsov on col.4, lines 15-20 and 48-53; discussing monitoring network communications comprises monitoring network communications in a network intrusion detection system component running in an execution context with the invoked application.

As per claim 25: See Gryaznov col.1, lines 32-36 and col.4, lines 32-41; discussing the operations further comprise providing an application-specific remedy for a detected intrusion.

As per claim 26: See Gryaznov col.1, lines 32-36 and col.4, lines 32-41; discussing providing an application-specific remedy comprises cutting at least a portion of the network communications for the invoked application.

As per claim 27: See Kouznetsov on col.4, lines 25-30 and col.6, lines 50-60; discloses requesting the application-specific intrusion criteria from the local repository; requesting the application-specific intrusion criteria from the master repository if the application-specific intrusion criteria is unavailable in the local repository; receiving the application-specific intrusion criteria from the master repository if requested; and receiving the application-specific intrusion criteria from the local repository.

As per claim 28: See Kouznetsov on col.5, lines 50-58; discussing examining the set of instructions comprises: applying a hash function to the set of instructions to generate a condensed representation; and comparing the condensed representation with existing condensed representations for known applications.

Conclusion

4. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435